SwA Benchmarking

March 09, 2010

Booz | Allen | Hamilton

Why measure???

"*The only man I know who behaves sensibly is my tailor; he takes my measurements anew each time he sees me. The rest go on with their old measurements and expect me to fit them*."

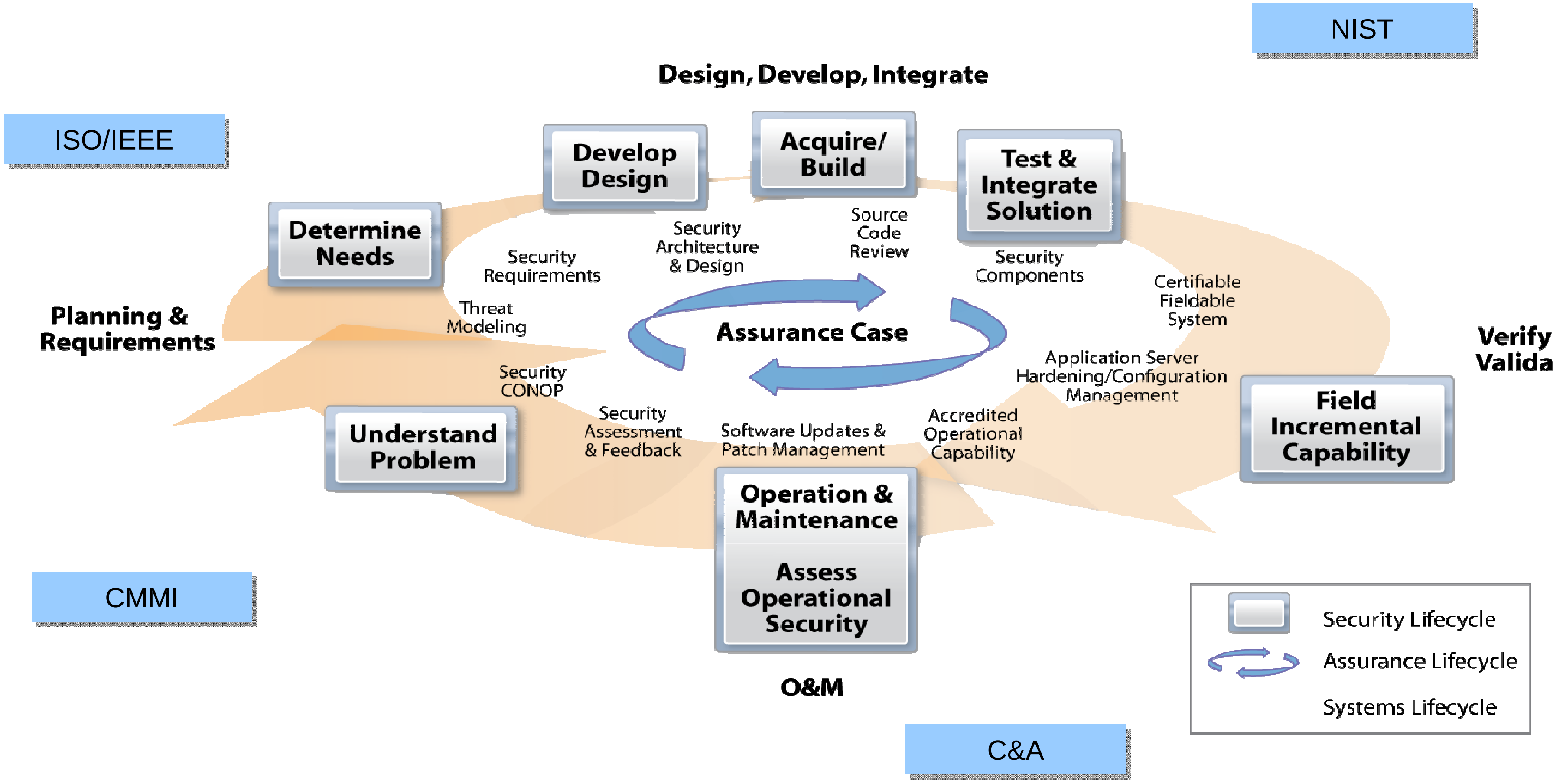
- George Bernard Shaw

Source: www.CartoonStock.com

Measures provide multiple benefits

- **Increase Accountability**
  - Help identify security controls that are implemented incorrectly, are not implemented, or are ineffective
  - Facilitate identification of the personnel responsible for security controls implementation
- **Improve Information Security Effectiveness**
  - Quantify improvements in securing information systems
  - Demonstrate quantifiable progress in accomplishing strategic goals and objectives
  - Determine the effectiveness of implemented information security processes, procedures, and security controls
- **Provide Quantifiable Inputs for Resource Allocation Decisions**
  - Contribute quantifiable information to the risk management process
  - Allow measurement of successes and failures of past and current information security investments
  - Provide a solid baseline for business case development
- **Demonstrate Compliance and Quality**
  - Appropriate measures and indicators of software artifacts such as requirements, designs, and source code can be analyzed to diagnose problems and identify solutions during project execution and reduce defects, rework (effort, resources, etc.), and cycle time.
  - These practices enable organizations to achieve higher quality products and reflect more mature processes, as delineated by the CMMI.

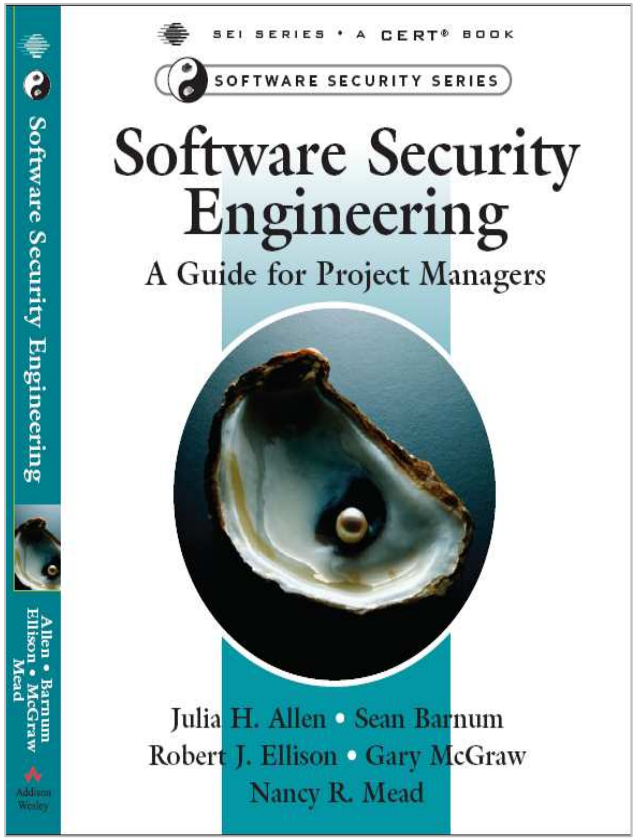
As a community use standards as shorthand to communicate and minimize risk


NIST
ISO/IEEE
CMMI
C&A
Design, Develop, Integrate
Develop Design
Acquire/ Build
Test & Integrate Solution
Determine Needs
Planning & Requirements
Security Requirements
Security Architecture & Design
Source Code Review
Security Components
Certifiable Fieldable System
Threat Modeling
Assurance Case
Verify & Validate
Security CONOP
Application Server Hardening/Configuration Management
Field Incremental Capability
Understand Problem
Security Assessment & Feedback
Software Updates & Patch Management
Accredited Operational Capability
Operation & Maintenance
Assess Operational Security
O&M
Security Lifecycle
Assurance Lifecycle
Systems Lifecycle

Booz | Allen | Hamilton

Software Security Engineering: A Key Resource

- **The book Software Security Engineering: A Guide for Project Managers** **http://www.softwaresecurityengineering.com/**
  - Contains an introduction to software security engineering and guidance for project managers
  - Inspired by the Build Security In website
  - Contributing authors are Julia Allen, Sean Barnum, Bob Ellison, Gary McGraw, and Nancy Mead
- **Six Main Practice Areas:**
  - Software security practices that span the SDLC
  - Requirements engineering practices
  - Architecture and design practices
  - Coding and testing practices
  - Security analysis for system complexity and scale: mitigations
  - Governance and management practices


SEI SERIES • A CERT® BOOK
SOFTWARE SECURITY SERIES
Software Security Engineering
A Guide for Project Managers
Julia H. Allen • Sean Barnum
Robert J. Ellison • Gary McGraw
Nancy R. Mead
Software Security Engineering
Allen • Barnum
Ellison • McGraw
Mead
Addison Wesley

The Adoption Of Swa Practices Has Been Baselined

Practices in Recommended Order	Description	Maturity	Audience	Relevant for These Roles
Secure coding practices	Use sound and proven secure coding practices to aid in reducing software defects introduced during implementation	L4	M, L	• Project manager • Security analyst • Developer
Source code review for security vulnerabilities	Perform source code review using static code analysis tools, metric analysis, and manual review to minimize implementation-level security bugs	L4	M, L	• Project manager • Security analyst • Developer

The content describes practices that have been successfully deployed and are in widespread use. Readers can start using these practices today with confidence. Experience reports and case studies are typically available.

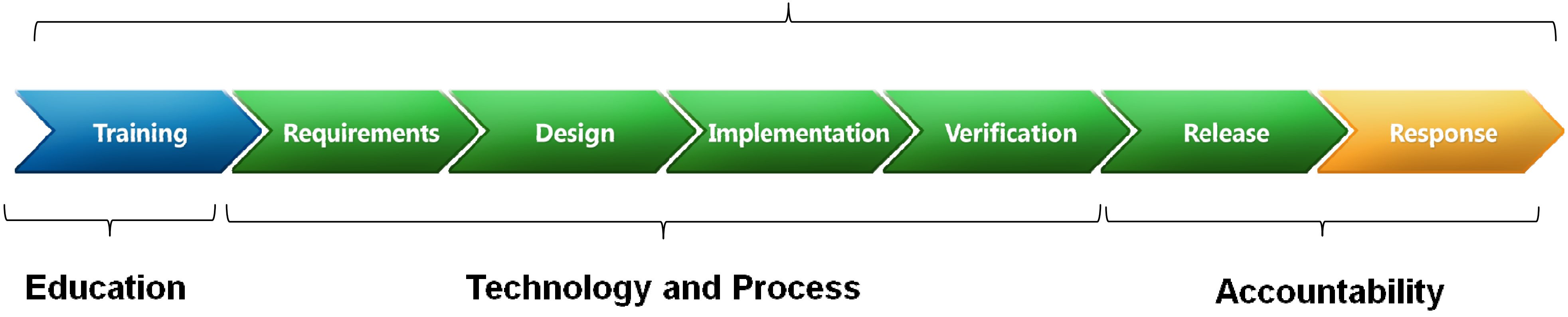
M - project and mid-level managers
L - technical leaders, engineering managers, first line managers, and supervisors

Adapted from: Software Security Engineering: How to Get Started Nancy Mead, SEI0

Microsoft Security Development Lifecycle (SDL)

Delivering secure software requires:

Executive commitment → SDL a mandatory policy at Microsoft since 2004



Training

Requirements

Design

Implementation

Verification

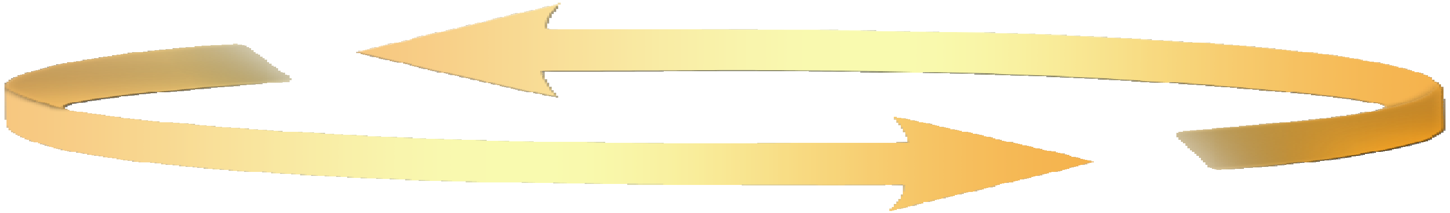
Release

Response

Education

Technology and Process

Accountability



Ongoing Process Improvements → 6 month cycle

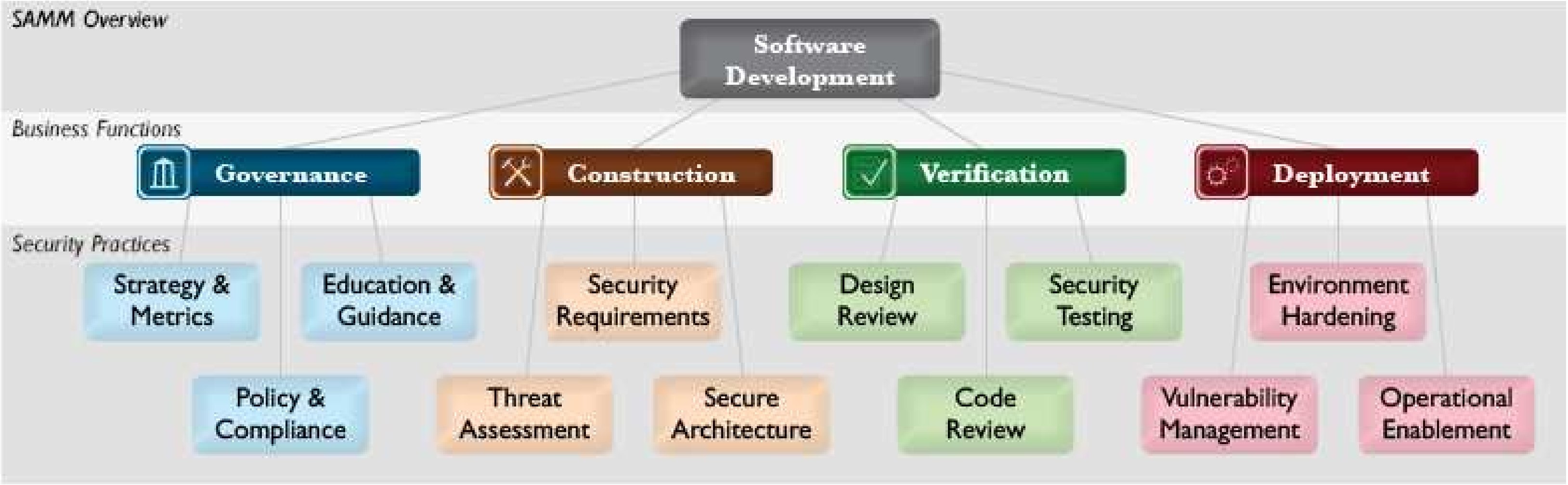
http://www.microsoft.com/sdl

BSIMM

- **Building Security In Maturity Model (BSIMM)**
  - http://www.bsi-mm.com/
  - Is designed to help understand and plan a software security initiative
  - BSIMM was created through a process of understanding and analyzing real-world data from nine leading software security initiatives
  - BSIMM uses a Software Security Framework (SSF), to provide a conceptual scaffolding for the model
  - Properly used, BSIMM can help determine where your organization stands with respect to real-world software security initiatives and what steps can be taken to make your approach more effective.
- **BSIMM**
  - Not a complete "how to" guide for software security, nor is it a one size fits all model
  - It is a collection of good ideas and activities that are in use today

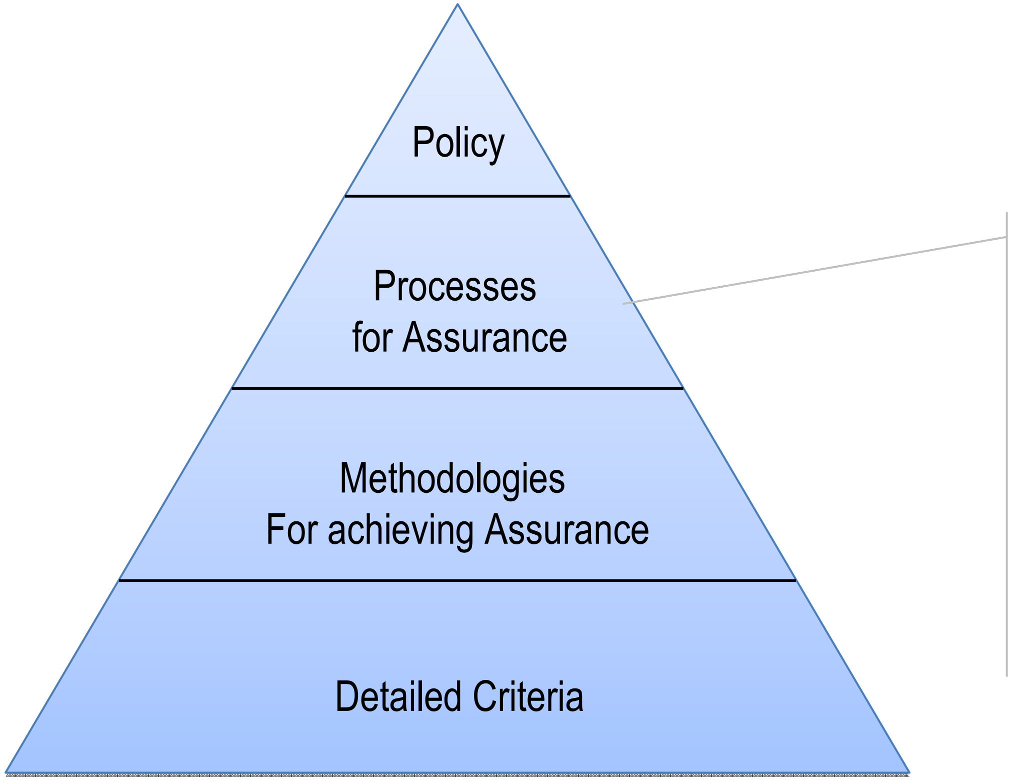
OPEN SAMM

- **Software Assurance Maturity Model (SAMM)**
  - http://www.opensamm.org/
  - Open framework to help organizations formulate and implement a strategy for software security tailored to specific risks



http://www.opensamm.org/downloads/SAMM-1.0.pdf

Assurance For CMMI® - A Framework For Organizational Improvement In Integrated Assurance



Project leadership and team members need to know where and how to contribute

Focus Topic: Assurance for CMMI ® defines the Assurance Thread for Implementation and Improvement of Assurance Practices

https://buildsecurityin.us-cert.gov/swa/procresrc.html

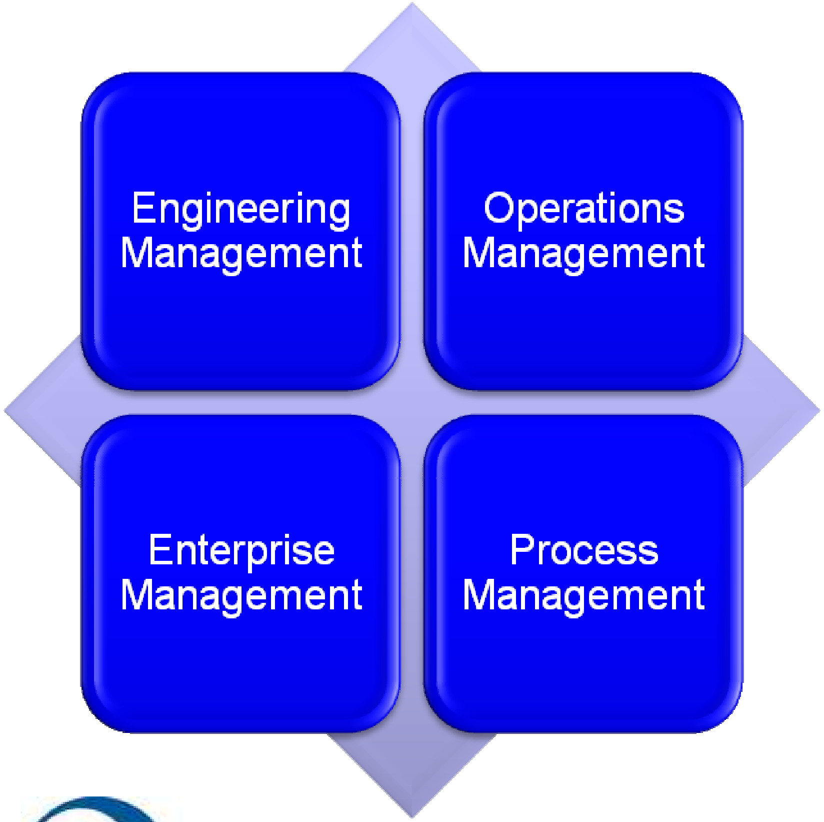
® Capability Maturity Model, Capability Maturity Modeling, and CMM are registered in the U.S. Patent & Trademark Office.

CERT® Resiliency Management Model

http://www.cert.org/resiliency/rmm.html

Requirements Management
RRD – Resiliency Requirements Development
RRM – Resiliency Requirements Management
Asset Management
ADM – Asset Definition and Management
Establishing Resiliency
CTRL – Controls Management
RTSE – Resilient Technical Solutions Engineering
SC – Service Continuity

Asset Resiliency Management
EC – Environmental Control
KIM – Knowledge & Information Management
PM – People Management
TM – Technology Management
Sourcing
EXD – External Dependencies
Threat, Incident, & Access Management
AM – Access Management
ID – Identity Management
IMC – Incident Management & Control
VAR – Vulnerability Analysis & Resolution



Governance, Risk, & Compliance
COMP – Compliance Management
EF – Enterprise Focus
RISK – Risk Management
Supporting Resiliency
COMM – Communications
FRM – Financial Resource Management
HRM – Human Resource Management
OTA – Organizational Training & Awareness

Data Collection & Logging
MON – Monitoring
Process Management
MA – Measurement and Analysis
OPD – Organizational Process Definition
OPF – Organizational Process Focus

CERT | Software Engineering Institute | Carnegie Mellon.

Adapted from "CERT® Resiliency Management Model", Lisa Young, SEI at the December 2009 SwA WGs

We Have Standards to Leverage for Benchmarking SwA Standards

Executive Dashboards

People

Policy and Mission/Business Goals

Risk Management

Acquisition Guidance

Business Case

Assurance Process Benchmarking

Tools to measure

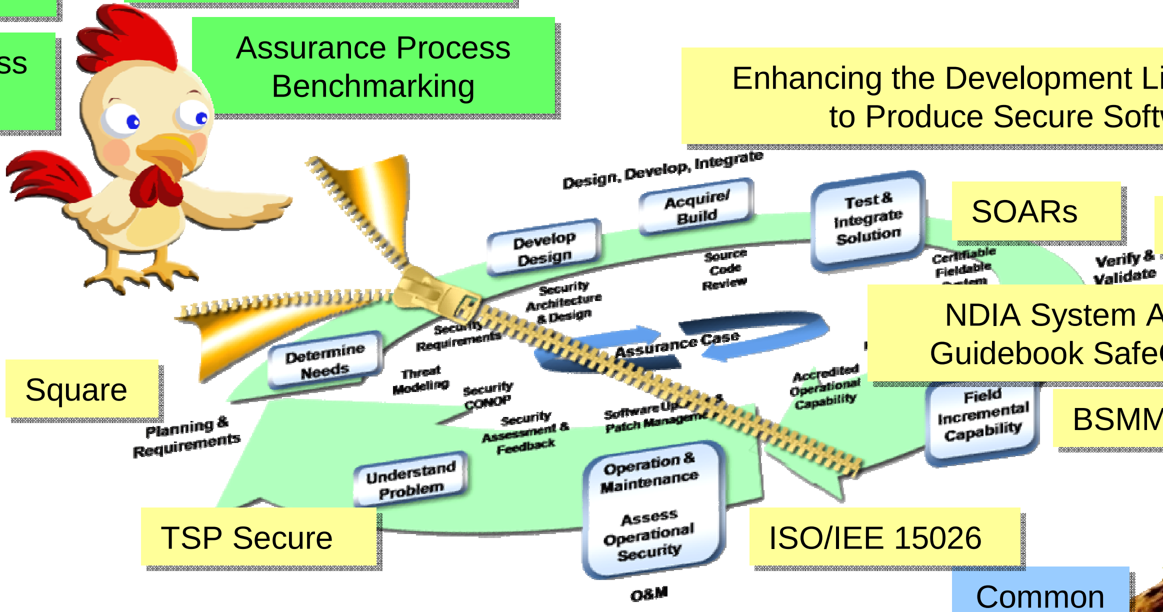
SAFEcode

IEEE

NIST

ISO

Enhancing the Development Life Cycle to Produce Secure Software


Design, Develop, Integrate
Develop Design
Acquire/ Build
Test & Integrate Solution
Source Code Review
Certifiable Fieldable System
Verify & Validate
Security Architecture & Design
Security Requirements
Assurance Case
Determine Needs
Threat Modeling
Security CONOP
Accredited Operational Capability
Field Incremental Capability
Planning & Requirements
Security Assessment & Feedback
Software Update & Patch Management
Understand Problem
Operation & Maintenance
Assess Operational Security
O&M

SOARs

Open SAMM

NDIA System Assurance Guidebook SafeCode WPs

Square

BSMM

Product labeling

Secure Code check lists

CWE

TSP Secure

ISO/IEE 15026

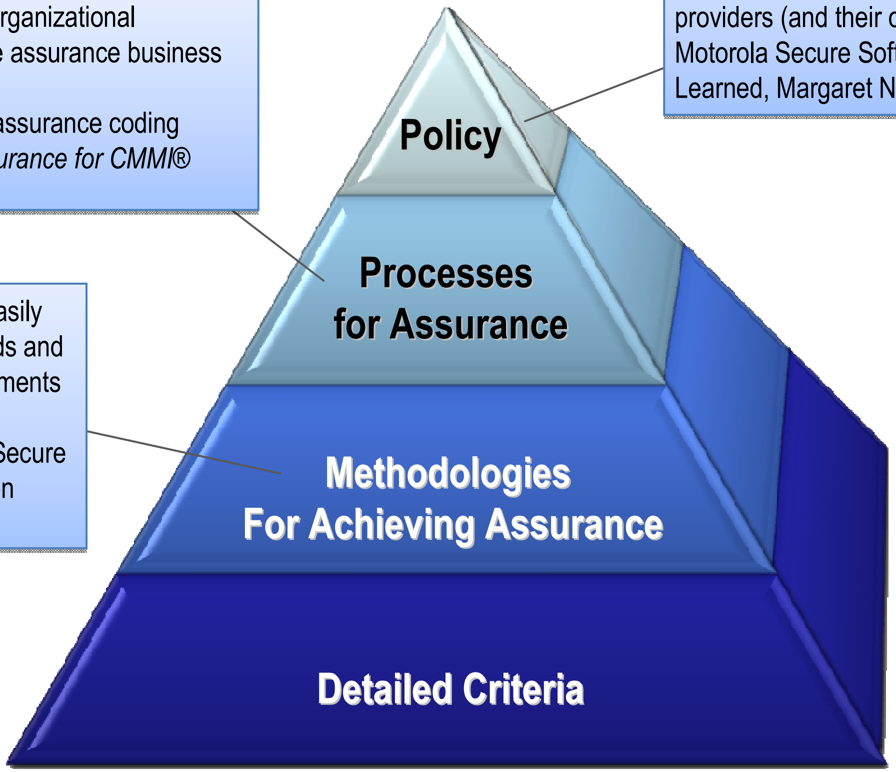
Common criteria

CVE

CAPEC

Static analysis tools

Measurement And Benchmarking At Multiple Levels Is Needed To Integrate, Communicate, And Improve Assurance Practices



"It is the policy of Motorola to offer security solutions designed to protect the confidentiality, integrity and availability of information and other assets appropriate to their value to Motorola, and to service providers (and their customers) using Motorola products." (source: Motorola Secure Software Development Model (MSSDM) Lessons Learned, Margaret Nadworny, August 10, 2007)

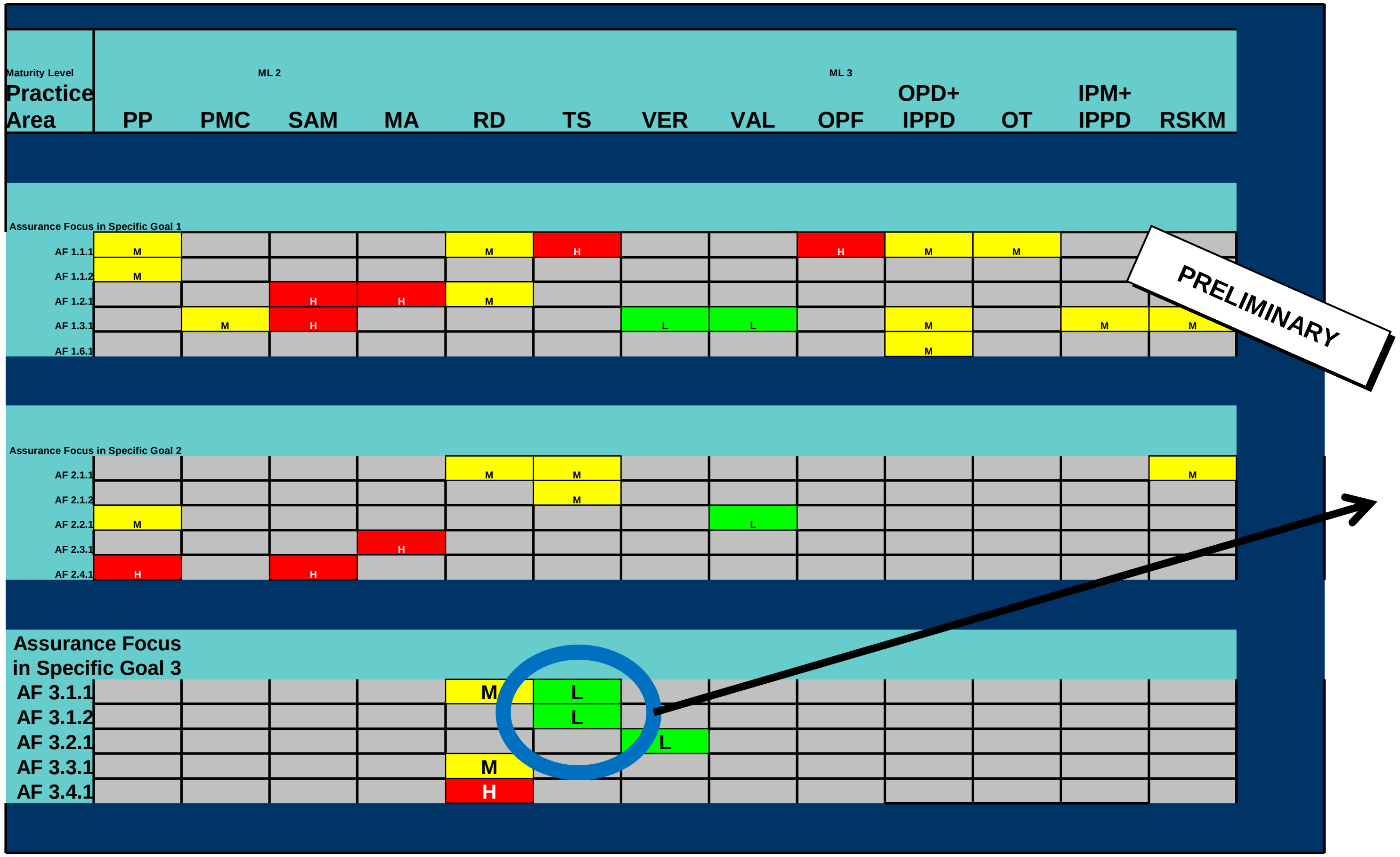
Establish and maintain organizational processes to achieve the assurance business objectives.
Identify deviations from assurance coding standards. *(Source: Assurance for CMMI® March 2009)*

BSIMSR Level 1: Provide easily accessible security standards and (compliance-driven) requirements
Safecode Whitepaper - Fundamental Practices for Secure SW Development (section on Programming)

TSP Secure CERT SCI provides language specific secure coding guidelines for C, C++, and Java.
To claim compliance with a standard, software developers must be able to produce on request documentation as to which systematic and specific deviations have been permitted during development.

Sample SwA Organizational Process Benchmarking Result

– Include assurance focus related findings in the respective process areas findings.



Maturity Level			ML 2						ML 3				
Practice Area	PP	PMC	SAM	MA	RD	TS	VER	VAL	OPF	OPD+ IPPD	OT	IPM+ IPPD	RSKM
Assurance Focus in Specific Goal 1													
AF 1.1.1	M				M	H			H	M	M		
AF 1.1.2	M												
AF 1.2.1			H	H	M								
AF 1.3.1		M	H				L	L		M		M	M
AF 1.6.1										M			
Assurance Focus in Specific Goal 2													
AF 2.1.1					M	M							M
AF 2.1.2						M							
AF 2.2.1	M							L					
AF 2.3.1				H									
AF 2.4.1	H		H										
Assurance Focus in Specific Goal 3													
AF 3.1.1					M	L							
AF 3.1.2						L							
AF 3.2.1							L						
AF 3.3.1					M								
AF 3.4.1					H								

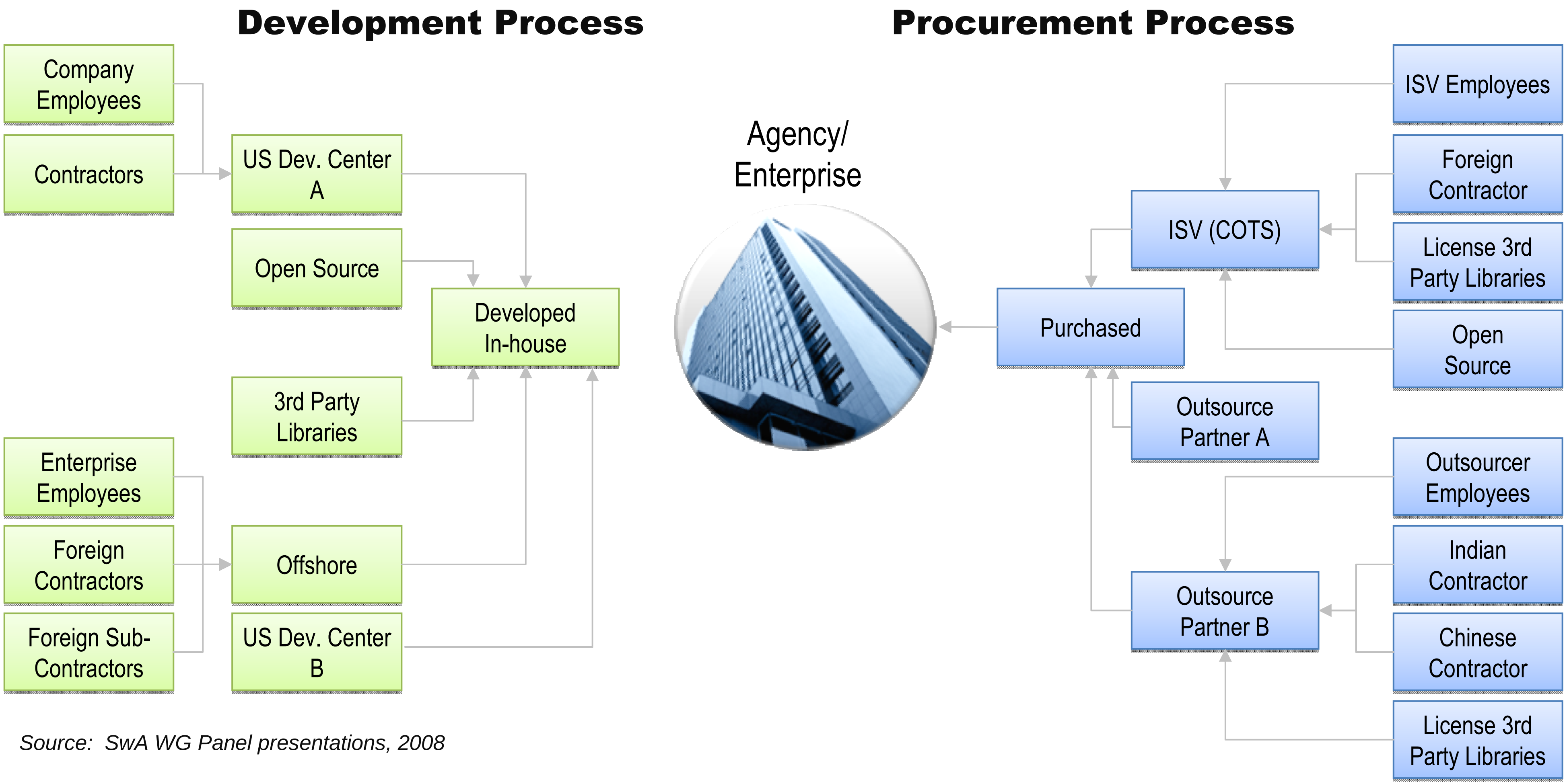
PRELIMINARY

TS AF 3.1.1 – Implement the assurance designs of the product component

TS AF 3.1.2 – Identify deviations from assurance coding standards. Implement appropriate mitigation to meet defined assurance objectives

Based on practice maturity in “Software Security Engineering: How to Get Started” Nancy Mead July 2007

Benchmarks Can Facilitate Understanding Risk Exposure And The Existence Of Swa Practices For Both The Supplier And Acquirer



Source: SwA WG Panel presentations, 2008

Contact Info

Michele Moss, CISSP, ISSPCS, CSSLP
Co-Chair DHS SwA Processes and Practices Working Group
moss_michele@bah.com